UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* information associated with david@terrapinfund.net stored at premises controlled by Zoho Corporation US, more fully described on Attachment A.	)	Case No.23-846M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 2/6/2023 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 1/23/2023 @ 2:55p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **david@terrapinfund.net** that is stored at premises owned, maintained, controlled, or operated by Zoho Corporation US, 4141 Hacienda Drive, Pleasanton, CA 94588.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Zoho Corporation US, (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account January 1, 2021 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

1. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 United States Code, § 1341(wire fraud) involving David Braeger and occurring after January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records and information relating to defrauding investors by David Braeger through Terrapin Funding, LLC; CryptoNite, LLC; Pantera Feeder Fund Holdings, LLC; and Dead Space, LLC.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FDIC-OIG may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with david@terrapinfund.net stored at premises controlled by Zoho Corporation US, more fully described on Attachment A.

Case No.23-846M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. § 1341	Wire Fraud

The application is based on these facts:

See Affidavit in Support of Application and Search Warrant, incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sara Hager, Special Agent FDIC

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 1/23/2023

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, US Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Sara Hager, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain account stored at premises controlled by Zoho Corporation US ("Zoho"), an email provider headquartered at 4141 Hacienda Drive, Pleasanton, CA 94588. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Zoho to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Deposit Insurance Corporation – Office of Inspector General (FDIC-OIG), and have been so employed since April 2014. I am also assigned as a Task Force Officer on the White Collar Squad of the FBI Milwaukee Field Office. My duties as a Special Agent include investigating violations of federal law, including various white-collar crimes such as wire fraud, money laundering, mortgage fraud, bank fraud, and I have received training regarding numerous investigations of white-collar crimes.

3. As a Special Agent, I attended training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. My training included various aspects of criminal investigations, specifically dealing with criminal law, money laundering, wire fraud, bank fraud, and various investigative techniques. Additionally, I obtained the Chainalysis Cryptocurrency

Fundamentals Certification. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of arrest and search warrants.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code, § 1341(wire fraud) have been committed by David Braeger, who owned and controlled Terrapin Funding LLC. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. The information detailed in this affidavit is based on my personal knowledge and observations, bank records, business records, and witness statements. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these matters. The information in this affidavit does not include all of my knowledge and investigation into this case. These facts are presented for the sole purpose of establishing probable cause in support of the application for a search warrant.

8. This investigation has uncovered that David Braeger ("Braeger"), owner of Terrapin Funding, LLC; Pantera Feeder Fund Holdings, LLC; and Dead Space, LLC; marketed himself as a cryptocurrency advisor and solicited a $20,000 cryptocurrency investment from Victim 1. Instead of investing in cryptocurrency, Braeger used Victim 1's investment for personal expenditures. Braeger then lied about where Victim 1's money went and ultimately failed to fully repay Victim 1. Braeger utilized an email account -- david@terrapinfund.net -- to communicate with Victim 1 at [redacted]@gmail.com to perpetuate this fraud.

9. According to the Wisconsin Department of Financial Institutions, Terrapin Funding LLC was registered on November 17, 2020, and as of October 1, 2022, the entity status was listed as delinquent. Braeger was listed as the last known registered agent and its last known principal office was listed as 11431 North Port Washington Road, Suite 100, Mequon, Wisconsin. This is a commercial office building and bank records show that Braeger made monthly, reoccurring payments to this building with the bank records noting "Terrapin Funding/Braeger".

10. According to the Wisconsin Department of Financial Institutions, Dead Space, LLC was registered on May 28, 2019, and as of June 14, 2022, was administratively dissolved. Braeger was listed as the last known registered agent and its principal office was listed as 8016 North Poplar Drive, Milwaukee, 53217. Braeger is known to have resided at that address in the past.

11. According to the Wyoming Secretary of State, Pantera Feeder Fund Holdings LLC was registered on March 24, 2021, and the current status is listed as administratively dissolved with delinquent taxes. The commercial registered agent address is 30 N Gould Street, Suite 12079, Sheridan, WY 82801. Braeger had a Pantera Feeder Fund Holdings LLC business deposit account at JP Morgan Chase. The Business Depository Certificate for that account states that Pantera Feeder Fund Holdings was registered in Wyoming and that Braeger was the only managing

member.

12. The Terrapin Funding, LLC website advertises itself as Wisconsin's Premier Small Business Finance Company and Cryptocurrency Advisory Group. According to the Terrapin Funding, LLC website, the cryptocurrency advisory component was provided through a separate entity called CryptoNite, LLC. The website further claims that Terrapin Funding, LLC and their partners have financed over $100 million in business financing.

13. Victim 1 and Braeger we high school classmates. In or around summer 2021, they became reacquainted. Victim 1 was interested in investing in cryptocurrency and saw on Facebook that Braeger marketed himself to be knowledgeable and successful in cryptocurrency investing. Victim 1's initial conversation with Braeger was via Facebook, and their subsequent communications were through text message, phone calls, emails and in-person.

14. On an unknown date after Braeger and Victim 1 reconnected via Facebook, they met at a Milwaukee-area restaurant. During this meeting, Braeger told Victim 1 that he had an association with a cryptocurrency firm called Pantera, which Braeger used to invest in cryptocurrency. Braeger told Victim 1 that if Victim 1 invested with him, Braeger could guarantee a 20% return on Victim 1's investment. Braeger told Victim 1 that the returns could be as high as 50% - 100%. Braeger further told Victim 1 that Victim 1 could withdraw his investment at any time.

15. As part of this investigation, the cryptocurrency firm Pantera Capital Management LP doing business as Pantera Capital was queried as to their business relationship with Braeger. Pantera Capital Management LP, which appears to be a legitimate cryptocurrency investment firm, is registered in Delaware and headquartered in California. Pantera Capital is not affiliated with Pantera Feeder Fund Holdings LLC. A Pantera Capital representative stated that Braeger

has never made an investment with Pantera Capital and is not affiliated with any limited partner at Pantera Capital.

16. On or around June 11, 2021, which was approximately one week later after Braeger and Victim 1's initial in-person meeting, they met again at the same Milwaukee restaurant. Braeger suggested that Victim 1 invest $100,000 with him, which Victim 1 was unwilling to do. At the end of their meeting, however, Victim 1 agreed to make a $20,000 cryptocurrency investment with Braeger. At Braeger's direction, Victim 1 wrote a $20,000 check payable to Pantera Feeder Fund with the memo line "Dave cryptonite". Braeger told Victim 1 that he would invest the money in cryptocurrency and guaranteed an investment return.

17. On or around June 14, 2021, Braeger deposited Victim 1's check into his JP Morgan Chase Pantera Feeder Fund Holdings, LLC business account ending 1886. This account was opened on March 24, 2021, and Braeger is the only authorized signatory.

18. A review of bank records shows that none of Victim 1's investment was used for a cryptocurrency investment. Victim 1's funds were used for Braeger's personal expenditures such as utility payments, food, gas and an $8,000 check made payable to Individual 1. Based on the investigation to date, it is unclear if Individual 1 is an additional victim or co-conspirator. Additionally, Braeger transferred $8,200 of Victim 1's investment to his Wells Fargo Dead Space, LLC business account ending 4696. A review of those bank records shows that Braeger used these funds for personal expenditures at Amazon, liquor stores and for food.

19. On an unknown date after Victim 1 made his investment, Victim 1 inquired with Braeger on the status of his investment. Braeger informed Victim 1 that he had already made $7,000 in profit, for a total investment of $27,000. Victim 1 inquired with Braeger several more times on the status of his investment, but received no response, causing Victim 1 to become

suspicious.

20. Due to Victim 1's growing concern, he asked Braeger to send his entire $27,000 investment to Victim 1's personal cryptocurrency wallet. In response, on August 26, 2021, Braeger sent an email from his david@terrapinfund.net account to Victim 1 with the subject line "transaction confirmation". In that email, Braeger attached the cryptocurrency confirmation containing a transaction hash number 0x26e0990a1aa111c5c7123013546353087075O2f8b95730390d2e4c7aaa74020d. The receiving wallet was listed as 0x5e480E679b499B5CC0171806Fb4f869c415c55fa. This receiving wallet number in the email Braeger sent ostensibly confirmed that the funds had been sent to the same receiving wallet number Victim 1 had provided to Braeger. Based on this, Victim 1 initially believed Braeger had sent Victim 1 all of his money as Victim 1 had requested.

21. All cryptocurrency transactions are recorded on a public ledger, known as a blockchain. A blockchain contains list of transactions that are mathematically verified and can be viewed by anyone. The blockchain records every transaction in which an address successfully sends or receives cryptocurrency. Publicized transaction information include sending and receiving addresses, date and time stamp, amount, and a transaction hash, which is a unique identifier of the transaction. This data makes the existence of a transaction on the blockchain easily verifiable, although anonymous.

22. I researched the transaction hash that Braeger provided and discovered that the information Braeger provided to Victim 1 was false. While Braeger provided a valid transaction hash, the receiving wallet in Braeger's document did not match the receiving wallet listed on the blockchain. All of the data fields on Braeger's document (i.e. date, time, fee, confirmation, amount, block number, and gas price) were identical to the items listed for this hash on the

blockchain. According to the blockchain, however, Braeger sent the funds to an entirely different wallet address, which was 0xc76f85f10299c10920394ea7c1efa489ebe569e3. Victim 1 confirmed that was not his wallet address he sent Braeger.

23. Victim 1 became aware that Braeger altered the receiving wallet number when he asked his son compare the transaction hash number provided in Braeger's document to the blockchain. Victim 1's son similarly discovered that Braeger altered the receiving wallet on the document provided to Victim 1. Victim 1 then confronted Braeger about the fraudulent document, stating that he knew the document was falsified. Braeger denied falsifying the document, and denied misappropriating the money. Braeger told Victim 1 that he lost the funds due to making a mistake when he transferred the cryptocurrency.

24. In the months after Victim 1 discovered Braeger falsified the document, Victim 1 repeatedly asked Braeger to refund his investment. Braeger continually promised Victim 1 that he would be repaid. Instead, Braeger made repeated excuses about problems he had encountered that caused him not to be able to pay Victim 1 as promised.

25. Law enforcement interviewed Victim 1 and obtained a download of Victim 1's phone, which included some communications between Victim 1 and Braeger, including text messages and screenshots of several emails they exchanged. Because of the way the phone downloaded, law enforcement was unable to get a full native copy of Victim 1's email communications with Braeger.

26. On June 14, 2021, Braeger sent an email from his email account "david@terrapinfund.net" to Victim 1's email account "[redacted]@gmail.com" with the subject line, "from Dave Braeger". In this email, Braeger stated that he was going to wire Victim 1's investment to cryptocurrency cold storage firm River Finance. Victim 1 was to receive

confirmation of that transfer. Braeger wrote that he was going to speak with Pantera analysts about cryptocurrency market conditions and decide where to invest Victim 1's funds. Bank records show that Victim 1's investment was not wired to River Finance, but instead used for Braeger's personal purposes.

27. On August 26, 2021, Braeger sent an email from his email account "david@terrapinfund.net" to Victim 1's email account "[redacted]@gmail.com", with the subject line "transaction confirmation". Included in this email was the falsified document containing the fraudulent cryptocurrency receiving wallet address.

28. On August 27, 2021, Braeger sent an email from his email account "david@terrapinfund.net" to Victim 1's email account "[redacted]@gmail.com", with the subject line "Urgent message". This email was addressed to "All Adamant Holders[1]". It requested that recipients respond with confirmation that they had received their cryptocurrency transfer the previous day because one of the transfers was sent to the correct wallet address, but had not shown up in the wallet. This indicates that there may be additional victims of Braeger's cryptocurrency scheme.

29. On September 10, 2021, Braeger sent an email from his email account "david@terrapinfund.net" to Victim 1's email account "[redacted]@gmail.com", with the subject line "checks". In this email, Braeger claimed that he was liquidating three mutual funds totaling $20,000, which he would use to repay Victim 1. Text messages show that Victim 1 only received $4,000 from this alleged liquidation.

---

[1] Adamant Vault is a platform that helps cryptocurrency investors maximize income from yield farming. Yield farming is an investment strategy whereby investors deposit and pool their cryptocurrency to pursue investment gains such as through cryptocurrency lending.

30. Based on these communications and the investigation to date, there is probable cause to believe that evidence of Braeger's commission of wire fraud will be found in the email account "david@terrapinfund.net".

31. In general, an email that is sent to a Zoho subscriber is stored in the subscriber's "mail box" on Zoho's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Zoho's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Zoho's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

32. In my training and experience, I have learned that Zoho provides a variety of on-line services, including electronic mail ("email") access, to individuals and companies. Email metadata shows that Zoho is the Internet Service provider for "david@terrapinfund.net". Subscribers obtain an account by registering with Zoho. During the registration process, Zoho asks subscribers to provide basic personal information. Therefore, the computers of Zoho are likely to contain stored electronic communications (including retrieved and unretrieved email for Zoho subscribers) and information concerning subscribers and their use of Zoho services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. A Zoho subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Zoho. In my training and

experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

34. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

35. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

36. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline

information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

38. Based on the forgoing, I request that the Court issue the proposed search warrant.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Zoho. Because the warrant will be served on Zoho, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **david@terrapinfund.net** that is stored at premises owned, maintained, controlled, or operated by Zoho Corporation US, 4141 Hacienda Drive, Pleasanton, CA 94588.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Zoho Corporation US, (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account January 1, 2021 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

1. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 United States Code, § 1341(wire fraud) involving David Braeger and occurring after January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records and information relating to defrauding investors by David Braeger through Terrapin Funding, LLC; CryptoNite, LLC; Pantera Feeder Fund Holdings, LLC; and Dead Space, LLC.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FDIC-OIG may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Zoho, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Zoho. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Zoho, and they were made by Zoho as a regular practice; and

b. such records were generated by Zoho's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Zoho in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Zoho, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature